Creating a Protected Virtual Learning Space: A Comprehensive Strategy for Security and User Experience in Online Education

Mohan Sai Dinesh Boddapati[1], Sri Aravind Desamsetti[1], Karunasri Adina[1(✉)], Padma Jyothi Uppalapati[1], P T Satyanarayana Murty[2], and RajaRao P. B. V[2]

[1] Department of Computer Science and Engineering, Vishnu Institute of Technology, Bhimavaram 534202, Andhra Pradesh, India
karunasri.adina@gmail.com

[2] Department of Computer Science and Engineering, Shri Vishnu Engineering College for Women, Bhimavaram 534202, Andhra Pradesh, India

Abstract. The pandemic has a significant impact on how people conduct meetings, both in corporations and in schools. Online meetings have become a popular way to connect people from all over the world, lowering the expenses and time associated with travel. Various video conferencing systems and communication tools have aided in this trend towards online meetings. Many countries have moved to online classrooms as an alternative to traditional face-to-face instruction in the educational sector. It has also enabled educational institutions to adapt to changing circumstances and continue to educate students. One of the major concerns is security. As online platforms become more popular, the potential of infiltration activities such as hacking or unauthorized access increases. This study proposes a comprehensive strategy for improving security and user experience in online education. The framework focuses on detecting existing participants, detecting intruders, restricting intruders, and restricting abusive messages. It employs authentication mechanisms, user behaviour analysis, network monitoring, and machine learning algorithms to validate participant identities, differentiate legitimate users from prospective invaders, restrict unauthorized access, and promote courteous conversation. The framework proves its usefulness in minimizing security concerns and promoting a secure online learning environment through simulations and case studies.

Keywords: Intrusion detection · Abusive messages · BERT model

1 Introduction

1.1 Content Creation

Covid-19 is the most lethal virus in ages. It is spreading like wildfire, and the only way to stop it is through social isolation. Schools began offering online classes to comply with this rule [1]. It may have been challenging at first, but everyone finally adapted to

P. Pareek et al. (Eds.): IC4S 2023, LNICST 536, pp. 350–361, 2024.
https://doi.org/10.1007/978-3-031-48888-7_30

the concept. You cannot deny that online classes are far more convenient than traditional classes. You can dress as you choose, access the lesson from anywhere in the world, and record the class for future reference. The most significant advantage of having classes online is that you can record all of them and refer to them later when studying as shown in Fig. 1 [2].

Online programmers are less expensive because they eliminate the need to maintain a physical site. Institutes began investing in online tools that were far less expensive than maintaining big parts of their physical properties. We understand that many teachers and kids struggled to acclimatize to technology. Eventually, everyone learned and is now aware of the different functions of a laptop or computer. The best part about online education is that you be-come Tech Savvy, and there is always something new to learn.

Fig. 1. Online Meeting

Eventually, everyone learned and is now aware of the different functions of a laptop or computer. The parent largest disadvantage was the high cost of purchasing laptop computers. Many low income parents had to use their savings to purchase laptops, as it became vital for pupils to be able to attend classes with ease. Problems with the internet, computers not working, and a lack of electricity are just a few examples. These are some of the issues that kids and teachers frequently face and are powerless to address. There are no such options available. You cannot deny that school children are capable of exploiting the circumstance and being less attentive in class.

1.2 Related Work

Several studies have looked into the use of data and technology analysis to improve security in online meeting procedures. Using facial detection or fingerprint technology, algorithmic models for machine learning have been utilized to detect the abusive messages and block such intruders in online meetings.

Karim [1] stated that the Google Meet app was the most secure against cyber-attacks, followed by Microsoft Teams and, finally the Zoom app but they didn't detect the intruders in the online meetings. Abudhagir [11] comprises one of the best face detection

performances, as the images in the dataset are one shot learned it has the triplet loss which helps to avoid more unrelated example of pictures while passing through the convolutional sheets.

De la Cruz [2] presents a framework for raising awareness about the need for more robust security measures such as threat prevention, identification security, compliance with academic institution law, and ethical conduct to protect student personal information now and in the future.

Chen [6] uses a comprehensive evaluation technique to compare user experiences before and after the outbreak of COVID-19, and eventually determines how user's concerns about the online education platform have changed. This paper investigates the supporting abilities and response levels of online education platforms during COVID-19, and proposes corresponding measures to improve how these platforms function in terms of access speed, reliability, timely transmission technology of video information, course management, communication and interaction, and learning and technical support.

For deep face recognition, the Zulfiqar [5] pretrained CNN model and a set of hyper parameters are experimentally chosen. The usefulness of deep facial recognition in automated biometric identification systems is demonstrated by promising testing findings with an overall accuracy of 98.76%. With the use of lexicon-based encodings, Koufakou [9] investigates several applications for lexical characteristics and offers a thorough dataset evaluation that tack-les both in-domain and cross-domain abusive content identification.

Caselli [3] created a pre-trained BERT model for detecting abusive words in English. This model was trained using RALE, a huge dataset of Reddit comments in English from communities banned for being offensive, abusive, or hateful that we gathered and made public. Nobata [4] created a machine learning based solution that outperforms a state of the art deep learning strategy for detecting hate speech in online user comments from two do-mains[14].

On the basis of the current pre-trained language model, Huang [10] suggests a multi task framework (MFAE) combining abuse detection and emotion categorization to increase the algorithm's representational capacity. Founta [7] proposed a deep learning architecture that uses a wide range of available metadata and combines it with automatically derived hidden patterns inside tweet text to detect various abusive behavioral standards that are strongly interconnected.

1.3 Contributions

A few students exchange URLs to academic sessions/webinars/CREs with miscreants, who subsequently login to the meeting/sessions using the IDs or names of other recognized attendees. After entering the meeting, mischievous kids cause indiscipline, confusion, and use nasty abusive language to disrupt the entire conference.

The COVID Pandemic/Lockdown has caused students to be frustrated. It has also damaged their mental health, resulting in undesirable behaviors and actions that disrupt the entire class and the decorum of the session/academic activity. A few students exchange URLs to academic sessions/webinars/CREs with miscreants, who subsequently login to the meeting/sessions using the IDs or names of other recognized

attendees. After entering the meeting, mischievous kids cause indiscipline, confusion, and use nasty abusive language to disrupt the entire conference (as shown in Fig. 2).

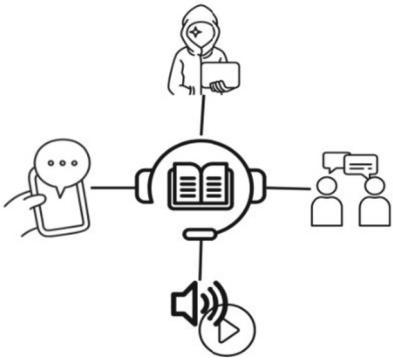

Fig. 2. Objectives of the work

Objective:

- Solutions need to be devised so that the intruders/miscreants are identified.
- They should not be able to use IDs and Names of the identified Participants/Students.
- It should get easy for the Host to block such intruders which does not happen usually.
- Messages (which are usually disturbing and offensive) need to be blocked in such a way that they are not shown in the chat box or displayed during the sessions.

2 Analysis

The effectiveness of teaching and learning, student involvement, technological utilization, and student success are all factors to consider while analyzing online classes. Here are some elements to consider when analyzing online classes:

- Learning outcomes: Providing excellent education and improving learning outcomes are two of the key goals of online classrooms. As a result, it is critical to assess the course's efficacy in delivering the desired learning outcomes. This can be accomplished by comparing student performance, like exam scores or assignment grades, to traditional in-person classes.
- Student engagement: Students must be self-motivated and proactive in their learning when taking online programmes. As a result, it is critical to assess the amount of student engagement in the course [16]. This can be accomplished by examining participation rates in class discussions, assignment and quiz completion rates, and overall attendance rates.
- Technology is frequently used in online classes to convey content and improve communication between professors and students. As a result, it is critical to assess the usefulness of the technology utilized in the course. This can include evaluating the online platform's dependability and functionality, as well as its usability for both instructors and students.

- Performance of the instructor: The role of the instructor is critical to the success of online classes. As a result, it is critical to evaluate the instructor's success in delivering course content, offering feedback and support, and building a collaborative learning environment.
- Student feedback: Finally, it is critical to collect feedback from students regarding their experiences in the course. Surveys or other forms of feedback mechanisms can be used to obtain insights on what worked well, what could be improved, and suggestions for future improvements.

Overall, online course analysis necessitates a thorough examination of all components of the course in order to establish its efficacy and identify opportunities for improvement. It is critical to collect data from many sources and stakeholders in order to acquire a comprehensive picture of the course and its impact on student learning.

3 Working Methodology

3.1 Identifying Intruders

Using facial detection or fingerprint technology [5] to identify intruders is a typical strategy used for access control and security. Here's a quick rundown of how it works:

- Facial Detection: Facial detection systems record and analyze the distinctive aspects of a person's face using cameras and specialized software. This technology can recognize certain facial characteristics such as the distance between the eyes, nose shape, and facial curves. Against find a match, these characteristics are matched against a database of authorized individuals.

  Face pattern recognition in machine learning is a multi-step process. First, a dataset of facial images is compiled, comprising both positive and negative examples of faces and non-face images. To maintain uniformity, preprocessing procedures such as scaling and normalization are used. To extract relevant facial features, feature extraction methods such as Haar cascades, HOG, or deep learning based approaches such as CNNs [11] are used. These features, together with the labels associated with them, are then used to train a machine learning model, such as SVM or KNN. A distinct dataset is used to evaluate the trained model's accuracy and performance. This procedure allows the ML model to recognize facial patterns and identify faces with a high degree of accuracy.
- Fingerprint identification: To identify people, fingerprint identification technology employs unique patterns and ridges on their fingertips. Fingerprint scanners take an image or sequence of images of the ridges on a person's finger and compare them to a database of authorized fingerprints.

  In machine learning, finger pattern recognition follows a similar procedure. A dataset of fingerprint pictures is compiled, including a wide range of samples from various individuals. To separate the fingerprint pattern, preprocessing techniques such as picture enhancement and segmentation are used. The fingerprint photos are used to extract distinguishing information such as ridge orientation and minutiae (ridge ends, bifurcations). These extracted features and labels are used to train machine learning models or statistical models such as HMMs or Neural Networks. The trained

models are then assessed using different validation or test images and metrics such as FAR, FRR, or EER. This allows the machine learning model to recognize and match fingerprint patterns, allowing for more accurate fingerprint recognition.

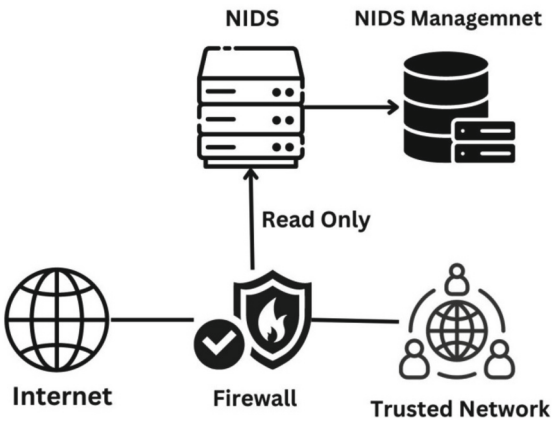

Fig. 3. Identifying Intruders in meetings

Both facial detection and fingerprint recognition systems give an extra degree of protection to the classroom by ensuring that only authorized personnel have access to it as shown in Fig. 3. These technologies are frequently utilized to improve security and prevent unauthorized entrance in a variety of industries, including education, government, and corporate environments.

3.2 Detecting Existing Participants

The following actions can be taken to recognize existing meeting attendees based on their email addresses and alert both the existing participant and the meeting organizer:

- Registration and Email Association: Each participant is needed to register for the meeting or class by entering their email address. Each participant's email address acts as a unique identification.
- Participant Database: Maintain a database that contains the email addresses of all registered attendees for the meeting or class.
- Participant Verification: When a participant enters a meeting, the meeting platform collects or extracts their email address.
- Email Address Comparison: The system compares the joining member's email address to the email addresses in the participant database.
- Detection and Notification: A pop-up notification is given to both the existing participant and the meeting organizer if a match is identified, indicating that the person already exists in the meeting or class.
- Existing Participant message: A pop-up message informs the existing participant that another participant with the same email address is attempting to join the meeting.

- Organizer Alert: A pop-up or alert notifies the meeting organizer that there are two participants in the meeting with the same email address. This advises the organizer to take appropriate action, such as validating the participants' identity or dealing with the problem.

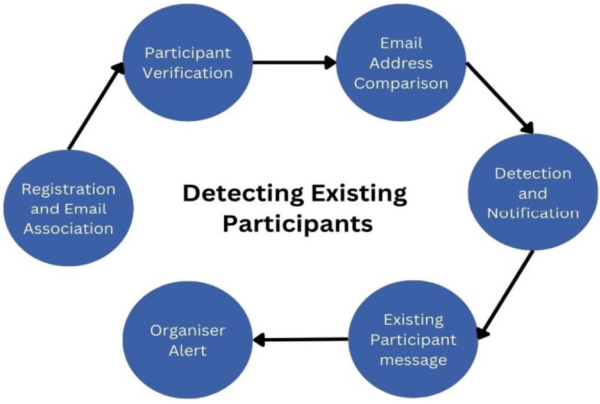

Fig. 4. Detecting Existing participants in online meetings

By following this procedure as shown in Fig. 4, both the present participant and the meeting organizer are notified of the potential duplicate participant as soon as possible. This allows the organizer to investigate and resolve any concerns linked to several participants using the same email address, maintaining the meetings or classes integrity and security.

3.3 Block Intruders

Various techniques can be used to prevent intruders and manage participant behavior during a lesson [12]. Here's an outline on how to deal with these issues:

Microphone use in class is critical for supporting good communication and engagement. Participants can express themselves, ask questions, and participate in discussions. However, in order to avoid disturbances and preserve a constructive learning environment, microphone usage must be managed. When participants should mute or un mute their microphones, instructors or meeting organizers can establish guidelines. Background noise and unexpected interruptions can be reduced by muting participants by default at admission and allowing them to un mute themselves when they want to contribute. Moderators can also actively monitor microphone usage and urge students to quiet themselves when not speaking, guaranteeing clear and focused audio throughout the session.

Video content in a class can boost engagement and promote a sense of community among students. Visual clues, nonverbal communication, and the sharing of pertinent materials are all possible. However, in order to create a focused and appropriate learning environment, video content must be managed. Video permissions can be controlled by

the meeting organizer or designated moderator, ensuring that only authorized attendees have video access. Monitoring the video feeds of participants during the lesson also aids in identifying any instances of irrelevant or inappropriate content being broadcast. To protect the integrity and relevance of the class content while allowing participants to offer relevant visual contributions, prompt action, such as eliminating disruptive videos or disabling video sharing, can be taken.

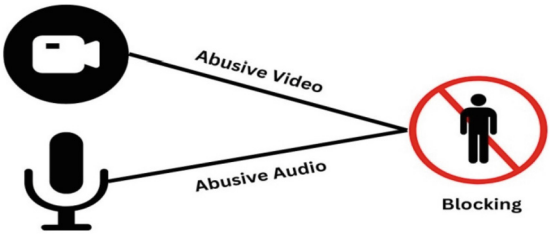

Fig. 5. Blocking intruders in meeting

Machine learning algorithms can be used in meetings to recognize irrelevant or off-topic spoken content and video, ensuring that discussions remain relevant and focused as shown in Fig. 5. The procedure entails assembling a collection of audio recordings and video feeds from meetings, which includes both linked and unconnected pieces. Noise reduction and frame extraction are two examples of preprocessing processes used on audio and video data. The audio and video streams are then analyzed to extract relevant information.

Classification algorithms or deep learning networks are taught using the retrieved characteristics and labels that indicate whether the segments are related or unrelated. These algorithms learn the properties and patterns of unrelated speech and video information. A different dataset is used to evaluate the trained models' performance in reliably detecting unrelated parts. Meeting systems or applications that use this ML-based method can automatically analyze both spoken content and video streams, indicating unconnected segments in real-time. This allows participants and organizers to stay focused and keep meetings on track, resulting in more productive and efficient talks.

3.4 Block Abusive Messages

A method for addressing abusive communications can be established to maintain a courteous and secure environment in the chat box during a meeting or class [14]. When an abusive message is discovered, the system warns the responsible person, reminding them of proper behavior. This initial warning provides the participant with an opportunity to correct their actions. If the abusive behavior continues, the system will take more serious action. The participant may be barred from further communications or perhaps removed outright from the meeting. This proactive strategy guarantees that abusive communications are addressed as soon as possible, while also promoting a good and inclusive learning environment for all participants.

It is critical to keep track of participant information and activities in order to retain responsibility and facilitate future action, if necessary. The system records pertinent information such as the participant's name, the time of the abusive communication [4], and any measures taken, such as warnings, blocks, or deletions. These log files provide a thorough record of participant behavior, which is useful evidence if additional inquiry or intervention is required. Meeting organizers and administrators can efficiently address instances of abusive messages, protect participants' well-being, and ensure a productive and courteous learning experience by logging participant information.

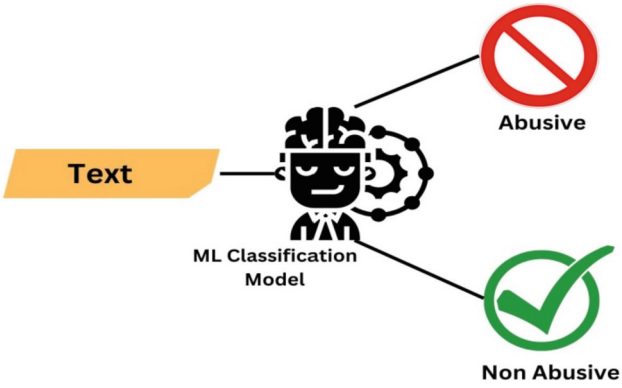

Fig. 6. Blocking abusive messages using BERT model

Using the BERT [8] model to determine whether a message is normal or abusive (as shown in Fig. 6) necessitates the use of natural language processing techniques. BERT (Bidirectional Encoder Representations from Transformers) is a sophisticated pre-trained language model that can be modified for a variety of NLP applications such as text categorization.

A labeled dataset is required to train a BERT [3] model for classifying normal and abusive texts. This dataset should include both typical and abusive message instances. To prepare the text data for entry into the BERT model, preprocessing processes such as tokenization and padding are used. BERT is then fine-tuned using labeled data, where the model learns to grasp the context and sentiment underlying the messages.

For BERT training we used Masked Language Model (MLM) approach Once fine-tuned, the BERT model that can be used to identify new messages as normal or abusive. The message is sent via the model (as shown in Fig. 7), which creates a forecast based on the training data's learnt patterns and context. To determine the classification, a threshold might be set, with a forecast above the threshold being abusive. The model's performance is assessed using metrics such as accuracy, precision, recall, and F1 score, which are compared to the ground truth labels. The model can be monitored and updated on a regular basis to increase its accuracy and adapt to changing language patterns.

i) Our text is tokenized. We begin with text tokenization, just as we would with transformers. We will obtain three different tensors as a result of tokenization:

- input_ids

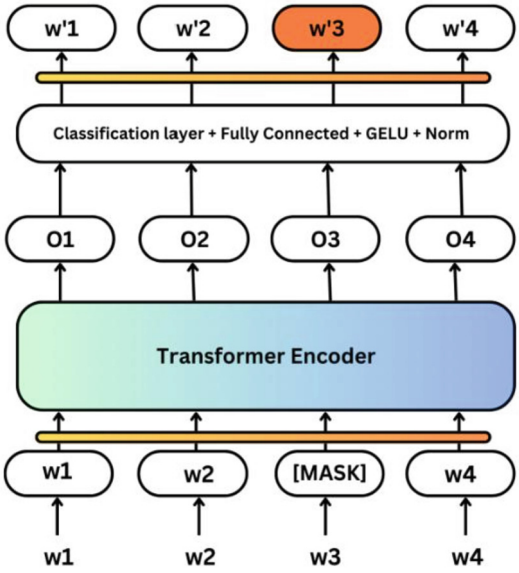

Fig. 7. Multiple layers of BERT model

- Token_type_ids
- attention_mask

ii) Make a tensor of labels. Because we're training our model here, we'll need a labels tensor to calculate loss — and optimize towards.

iii) Tokens in input_ids are masked. We can mask a random selection of tokens now that we've produced a duplicate of input_ids for labels.

iv) Determine your loss. We run the input_ids and labels tensors through our BERT model and compute the difference between them.

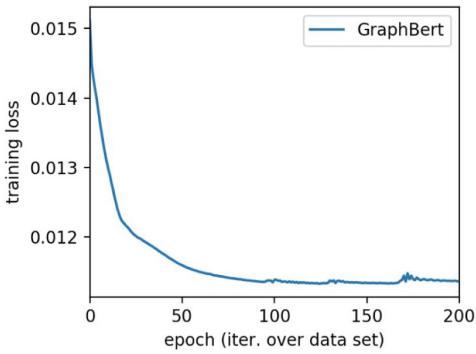

Fig. 8. Epoch vs Loss

A fine-tuned model may accurately identify communications as normal or abusive by exploiting BERT's (as shown in Fig 8) epochs vs training loss that has the ability to recognize contextual meaning. This can be implemented to a variety of applications, such as chat moderation, social media monitoring, or content filtering, to ensure that users are safe and polite.

4 Evaluation

The effectiveness of measures used to identify and prevent unauthorized access to the online class by those who are not authorized to attend is assessed during the evaluation of online class intruder tracking. Here are some variables to consider while evaluating online class intruder tracking:

- False positive: False positives occur when people are mistakenly detected as intruders. As a result, it is critical to assess the tracking system's false positive rate, which may be done by comparing the number of false positives to the total number of attempted logins.
- Response time: When an intruder is spotted, it is critical to act swiftly to prevent them from gaining access to the class. As a result, it is critical to assess the tracking system's response time, which may be accomplished by evaluating the time it takes for the system to recognize an intruder and take action to prevent them from entering the class.
- User experience: The tracking system should not interfere with legitimate users' experiences. As a result, it is critical to assess the tracking system's impact on legitimate users, such as whether it creates delays or necessitates additional authentication processes.
- Effectiveness of prevention measures: Aside from detecting and stopping intruders, it is critical to assess the effectiveness of prevention measures in place to detect possible intruders. This can include things like demanding strong passwords or two-factor authentication, which can be measured by the frequency of successful unauthorized attempts.

Overall, evaluating online class intruder tracking necessitates a thorough examination of numerous elements in order to determine its efficiency in preventing unauthorized access to the class. It is critical to regularly monitor and update the tracking system in order to resolve any vulnerabilities or weaknesses and ensure the online class environment's security.

5 Conclusion

Intruder tracking is a critical component of assuring the security and integrity of online learning environments. The tracking system is designed to detect and prevent unauthorized access to the class by people who are not authorized to be there. The efficiency of the procedures employed to identify and prevent unauthorized access to the class is assessed during the evaluation of online class intruder tracking. The detection rate, false positive rate, reaction time, user experience, and effectiveness of preventative measures are all factors that can be examined when evaluating online class intruder surveillance.

It is critical to monitor and update the tracking system on a regular basis in order to fix any vulnerabilities or weaknesses and ensure the security of the online learning environment for all genuine users. Finally, a good online class intruder tracking sys-tem can improve overall class effectiveness and promote a safer learning environment for all students and instructors.

References

1. Karim, N.A., Ali, A.H.: E-learning virtual meeting applications: a comparative study from a cybersecurity perspective. Indonesian J. Electr. Eng. Comput. Sci. **24**(2), 1121–1129 (2021)
2. De la Cruz, J.: Online Class: Student Data Privacy. Int. J. **10**(7) (2022)
3. Caselli, T., et al.: HateBERT: retraining BERT for abusive language detection in English. arXiv preprint arXiv:2010.12472 (2020)
4. Nobata, C., et al.: Abusive language detection in online user content. In: Proceedings of the 25th International Conference on World Wide Web (2016)
5. Zulfiqar, M., et al.: Deep face recognition for biometric authentication. In: 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). IEEE (2019)
6. Chen, T., et al.: The impact of the COVID-19 pandemic on user experience with online education platforms in China. Sustainability **12**(18), 7329 (2020)
7. Founta, A.M., et al.: A unified deep learning architecture for abuse detection. In: Proceedings of the 10th ACM Conference on Web Science (2019)
8. Hugging Face. BERT 101. Retrieved from http://www.springer.com/lncs
9. Koufakou, A., et al.: HurtBERT: incorporating lexical features with BERT for the detection of abusive language. In: Proceedings of the Fourth Workshop on Online Abuse and Harms. Association for Computational Linguistics (2020)
10. Huang, Y., et al.: A multitask learning framework for abuse detection and emotion classification. Algorithms **15**(4), 116 (2022)
11. Abudhagir, U.S., Anuja, K., Patel, J.: Faster RCNN for face detection on a FaceNet model. In: Vijayanand, R., Devaraj, D., Kannapiran, B. (eds.) Advances in Mechanical and Materials Technology: Select Proceedings of EMSME 2020, pp. 283–293. Springer Singapore (2022) https://doi.org/10.1007/978-981-16-2794-1_25
12. Vijayanand, R., Devaraj, D., Kannapiran, B.: Support vector machine-based intrusion detection system with reduced input features for advanced metering infrastructure of the smart grid. In: 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE (2017)
13. Bushetty, S., et al.: Analysis of Online Comments Using Machine Learning Algorithms
14. Subbarao, M. V., Padavala, A. K., & Harika, K. D.: Performance Analysis of Speech Command Recognition Using Support Vector Machine Classifiers. In Communication and Control for Robotic Systems, pp. 313-325. Springer Singapore (2021).
15. Bonthu, S., Dayal, A.: Maximizing student engagement by integrating social media in assignments of an online course. J. Eng. Edu. Transformations, 35(Special Issue 1) (2022)